UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/699,947	11/03/2003	Sajosh Janarthanam	PJW181	4353

7590 02/22/2007

Paul J. Winters
307 Cypress Point Drive
Mountain View, CA 94043

EXAMINER	
LEMMA, SAMSON B	
ART UNIT	**PAPER NUMBER**
2132	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	02/22/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	**Application No.** 10/699,947	**Applicant(s)** JANARTHANAM ET AL.	
	Examiner Samson B. Lemma	**Art Unit** 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03 November 2003*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-3 and 5-10* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3 and 5-10* is/are rejected.

7)☒ Claim(s) *4,11 and 12* is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

1. **Claims 1-12** have been examined.

Priority

2. This application does not claim priority of an application. Therefore, the effective filling data for the subject matter defined in the pending claims of this application is **11/03/2003.**

Claim Objections

3 Claim 8 is objected to because of the following informalities: Dependent claim 8 depends on itself. For the purpose of examination, it is assumed that it depends on independent claim 7.

Appropriate correction is required.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. **Claims 1-3 and 5-10** are rejected under 35 U.S.C. 103(a) as being unpatentable over admitted prior art (hereinafter referred to as **Admission**) (Provided Specification) in view of **Richard Ferrant** (hereinafter referred as **Ferrant**) (U.S. Patent No 6,421,799 B1) (Date of Patent: July 16, 2002)

6. **As per independent claims 1, Admission discloses a method of testing a device** *[Title "testing the encryption function device" or see also on page 1, "DUT"/device under the test")* **comprising:**

- **Providing a first data string** *[Page 2, lines 14-18, "P1S1", see also figure 1, ref. Num "P1S1"];*
- **Providing a second data string in a memory structure [page 2, lines 26-36 and figure 3, ref. Num "eP1S2"];**
- **Encrypting the first data string** *[See figure 1, ref. "P1S1"]* **using an encryption algorithm** *[see page 2, lines 14-18, "AES"],* **to provide an encrypted data string;** *[Page 2, lines 14-18, "eP1S1", see also figure 1, ref. Num "eP1S1"];*

and

- **Comparing a characteristic of the encrypted data string with a characteristic of the second data string.[page 6, lines 14-19]** *(" While it would be of course desirable to test the encryption function of the DUT for proper operation thereof, i. e., that the encrypted packet data string is as expected, the **matching of resulting encrypted packet data segment against each of the possible encrypted forms is impractical,** because of the very large number of possible encrypted forms. Therefore, what is needed is a method for testing the encryption function of a device, which method is simple and effective in use.")*
- Admission does not explicitly disclose,

Comparing a characteristic of the encrypted data string with a characteristic of the second data string.

However, in the field of endeavor **Ferrant**, discloses way of testing the proper manufacturing of a ROM consists of reading its content and checking that all the stored information is correct. This test operation is lengthy and expensive, and an embarked testing device is included in a ROM. Such a device is designed for, during a test phase, successively receiving all the data stored in the memory, **adding them, multiplying them, etc. according to an adequate encryption algorithm, and comparing the final result with the result expected from the memory data.** When the results are equal, the memory is assumed to be good, which meets the limitation of "comparing **a characteristic of the encrypted data string with a characteristic of the second data string."** *[Column 1, lines 8-33]*

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to combine the feature of comparison as per teachings of **Ferrant**, in to the method as taught by Admission, in order to provide effective testing mechanism. [See column 1, lines 18-35]

7. **As per independent claims 6-7, Admission discloses a** **method of testing a device** *[Title "testing the encryption function device" or see also on page 1, "DUT"/ device under the test")* **comprising:**

- **Providing a first data string** *[Page 2, lines 14-18, "P1S1", see also figure 1, ref. Num "P1S1"];*
- **Providing a second data string in a memory structure [page 2, lines 26-36 and figure 3, ref. Num "eP1S2"];**
- **Encrypting the first data string** *[See figure 1, ref. "P1S1"]* **using an encryption algorithm** *[see page 2, lines 14-18, "AES"],* with an initialization vector applied in such encryption,*[Page 2, lines 14-18, see initialization vector "IVAES1", see also figure 1, ref. "IVAES1")* **to generate an encrypted data string;** *[Page 2, lines 14-18, "eP1S1", see also figure 1, ref. Num "eP1S1"];* **and**
- **Comparing an initialization vector associated with the encrypted data string with an initialization vector applied in encrypting the first data string.[page 6, lines 14-19]** *(" While it would be of course desirable to test the*

encryption function of the DUT for proper operation thereof, i. e., that the encrypted packet data string is as expected, the ***matching of resulting encrypted packet data segment against each of the possible encrypted forms is impractical,*** *because of the very large number of possible encrypted forms. Therefore, what is needed is a method for testing the encryption function of a device, which method is simple and effective in use.")*

- Admission does not expressly disclose,

Comparing a characteristic of the encrypted data string with a characteristic of the second data string.

However, in the field of endeavor **Ferrant**, discloses way of testing the proper manufacturing of a ROM consists of reading its content and checking that all the stored information is correct. This test operation is lengthy and expensive, and an embarked testing device is included in a ROM. Such a device is designed for, during a test phase, successively receiving all the data stored in the memory, **adding them, multiplying them, etc. according to an adequate encryption algorithm, and comparing the final result with the result expected from the memory data.** When the results are equal, the memory is assumed to be good, which meets the limitation of "comparing **a characteristic of the encrypted data string with a characteristic of the second data string."** *[Column 1, lines 8-33]*

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to combine the feature of comparison as per teachings of **Ferrant**, in to the method as taught by Admission, in order to provide effective testing mechanism. [See column 1, lines 18-35]

8. **<u>As per dependent claims 2-3 and 8-10, the combination of Admission and Ferrant discloses a</u> method as applied to claims above. Furthermore, Admission discloses the method wherein, the step of comparing a characteristic of the**

encrypted data string with a characteristic of the second data string comprises comparing the bit length of the encrypted data string with the bit length of the second data string. [page 1, line 16, page 6, lines 14-19] *(" While it would be of course desirable to test the encryption function of the DUT for proper operation thereof, i. e., that the encrypted packet data string is as expected, the* ***matching of resulting encrypted packet data segment against each of the possible encrypted forms is impractical,*** *because of the very large number of possible encrypted forms. Therefore, what is needed is a method for testing the encryption function of a device, which method is simple and effective in use." And on page 1, lines 16 of the applicant's specification discloses that the properties of the data* ***packets includes packet length)***

9. **<u>As per dependent claim 5, the combination of Admission and Ferrant discloses a</u> method as applied to claims above. Furthermore, Admission discloses the method wherein, the data string in the memory structure is an unencrypted data string.** *[See figure 1, ref, "P1S1" and figure 2, ref. "P1S2"]*

Allowable Subject Matter

10. **<u>Claims 4 and 11-12</u>** are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

11. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.(See PTO-Form 892).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Samson B Lemma whose telephone number is 571-272-3806. The examiner can normally be reached on Monday-Friday (8:00 am---4: 30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, BARRON JR GILBERTO can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-873-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

SAMSON LEMMA
S.L.
02/10/2007

Benjamin E. Lanier
Examiner AU 2132